Amendments to the Claims

1. (Currently Amended) A method comprising:

generating a plurality of protection policy descriptors during a pre-boot environment;

assigning each of the plurality of protection policy descriptors to a respective one of a plurality of memory ranges during the pre-boot environment, wherein each of the protection policy descriptors is indicative of a corresponding protection policy for its one of the memory ranges;

storing the protection policy descriptors in a resource protection list; and

storing the resource protection list in a location accessible in a post-boot environment.

2. (Previously Presented) A method as defined in claim 1, further comprising initializing each of the memory ranges during the pre-boot environment to be a firmware resource.

3. (Currently Amended) A method as defined in claim 1, further comprising, for each protection policy descriptor, generating at least one hash code based on that protection policy descriptor.

4. (Original) A method as defined in claim 3, further comprising storing the at least one hash code in a trusted protection module platform configuration register.

5. (Currently Amended) A method as defined in claim 1, further comprising storing the protection policy descriptors in an advanced configuration and power interface differentiated system descriptor table.

6. (Previously Presented) A method as defined in claim 1, wherein each of the memory ranges includes at least one of a register region, a firmware data memory region, a firmware code memory region, or a hand-off information memory region.

7. (Previously Presented) A method as defined in claim 1, wherein the pre-boot environment comprises executing at least one of a basic input output system or an extensible firmware interface.

8. (Previously Presented) A method as defined in claim 1, wherein storing the resource protection list comprises storing the resource protection list in a location accessible by at least one of a secure virtual machine monitor or an operating system in the post-boot environment.

9. (Original) A method as defined in claim 1, further comprising establishing a resource protection policy in the post-boot environment based on the resource protection list.

10. (Original) A method as defined in claim 1, further comprising enabling the resource protection list to be validated in the post-boot environment.

11. (Currently Amended) An apparatus comprising:

a processor system; and

a memory communicatively coupled to the processor system, the memory including stored instructions that enable the processor system to:

generate a plurality of protection policy descriptors during a pre-boot environment,

assign each of the plurality of protection policy descriptors to a respective one of a plurality of memory ranges during the pre-boot environment, wherein each of the protection policy descriptors is indicative of a corresponding protection policy for its one of the memory ranges;

store the protection policy descriptors in a resource protection list, and

store the resource protection list in a location accessible in a post-boot environment.

12. (Previously Presented) An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to initialize each of the memory ranges during the pre-boot environment to be a firmware resource.

13. (Currently Amended) An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to, for each protection policy descriptor, generate at least one hash code based on that protection policy descriptor.

14. (Original) An apparatus as defined in claim 13, wherein the instructions stored in the memory enable the processor system to store the at least one hash code in a trusted protection module platform configuration register.

15. (Currently Amended) An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to store the protection policy descriptors in an advanced configuration and power interface differentiated system descriptor table.

16. (Previously Presented) An apparatus as defined in claim 11, wherein each of the memory ranges includes at least one of a register region, a firmware data memory region, a firmware code memory region, or a hand-off information memory region.

17. (Previously Presented) An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to execute at least one of a basic input output system or an extensible firmware interface in the pre-boot environment.

18. (Original) An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to store the resource protection list in a location accessible by a secure virtual machine monitor in the post-boot environment.

19. (Original) An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to enable the resource protection list to be validated in the post-boot environment.

20. (Original) An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to establish a resource protection policy in the post-boot environment based on the resource protection list.

21. (Currently Amended) A computer readable medium having instructions stored thereon that, when executed, cause a machine to:

generate a plurality of protection policy descriptors during a pre-boot environment;

assign each of the plurality of protection policy descriptors to a respective one of a plurality of memory ranges during the pre-boot environment, wherein each of the protection policy descriptors is indicative of a corresponding protection policy for its one of the memory ranges;

store the protection policy descriptors in a resource protection list; and

store the resource protection list in a location accessible in a post-boot environment.

22. (Previously Presented) A computer readable medium as defined in claim 20 having instructions stored thereon that, when executed, cause the machine to initialize each of the memory ranges during the pre-boot environment to be a firmware resource.

23. (Currently Amended) A computer readable medium as defined in claim 20 having instructions stored thereon that, when executed, cause the machine to generate each of the protection policy descriptors for at least one of a register region, a firmware data memory region, a firmware code memory region, or a hand-off information memory region.

24. (Currently Amended) A computer readable medium as defined in claim 20 having instructions stored thereon that, when executed, cause the machine to generate, for each protection policy descriptor, at least one hash code based on that protection policy descriptor.

25. (Original) A computer readable medium as defined in claim 24 having instructions stored thereon that, when executed, cause the machine to store the at least one hash code in a trusted protection module platform configuration register.

26. (Currently Amended) A computer readable medium as defined in claim 20 having instructions stored thereon that, when executed, cause the machine to store the protection policy descriptors in an advanced configuration and power interface differentiated system descriptor table.

27. (Previously Presented) A computer readable medium as defined in claim 20 having instructions stored thereon that, when executed, cause the machine to execute at least one of a basic input output system or an extensible firmware interface in the pre-boot environment.

28. (Original) A computer readable medium as defined in claim 20 having instructions stored thereon that, when executed, cause the machine to store the resource protection list in a location accessible by a secure virtual machine monitor in the post-boot environment.

29. (Original) A computer readable medium as defined in claim 20 having instructions stored thereon that, when executed, cause the machine to enable the resource protection list to be validated in the post-boot environment.

30. (Original) A computer readable medium as defined in claim 20 having instructions stored thereon that, when executed, cause the machine to establish a protection policy in the post-boot environment based on the resource protection list.

31. (Currently Amended) An apparatus comprising:

a processor system; and

a flash memory communicatively coupled to the processor system, the flash memory including stored instructions that enable the processor system to:

generate a plurality of protection policy descriptors during a pre-boot environment,

assign each of the plurality of protection policy descriptors to a respective one of a plurality of memory ranges during the pre-boot environment, wherein each of the protection policy descriptors is indicative of a corresponding protection policy for its one of the memory ranges;

store the protection policy descriptors in a resource protection list, and

store the resource protection list in a location accessible in a post-boot environment.

32. (Previously Presented) An apparatus as defined in claim 31, wherein each of the memory ranges includes at least one of a register area, a firmware data memory region, a firmware code memory region, or a hand-off information memory region.